УДК 343.1

© Ольга Виноградова
доцент кафедры криминалистики
Уральского юридического института МВД России
(г. Екатеринбург),
кандидат юридических наук

© Olga Vinogradova
Associate Professor of the Forensics dept.
of the Ural Law Institute of the Ministry
of Internal Affairs of Russia (Yekaterinburg),
Ph.D in Law

ОТДЕЛЬНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Компьютерные технологии стали неотъемлемой частью жизни каждого члена общества вследствие их повсеместного использования. Решение задач информационной безопасности в условиях современной социально-политической ситуации в нашей стране является одной из ключевых задач обеспечения жизнедеятельности общества, в первую очередь ввиду ценности информационных ресурсов в настоящее время. Грамотное решение задач в области информационной безопасности напрямую зависит от применяемой политики безопасности: необходимо учитывать все аспекты технологического процесса обработки информации для того, чтобы наиболее уязвимые объекты были максимально защищены при появлении преступника.

Основной тенденцией XXI века является всеобщая цифровизация процессов и появление цифровой продукции, что напрямую влияет на экономическое благополучие государства и проявляется в таких макропроцессах, как цифровая экономика. Указанное обуславливает направленность современных представлений о развитии государственных и правовых институтов в сторону внедрения электронных комплексов, цифровых массивов информации, интерактивных способов взаимодействия и способов защиты личности. В частности, Президент Российской Федерации В. В. Путин прямо указывает на необходимость наращивания темпов цифровой трансформации для достижения национальных целей развития [1].

Узкий и широкий подход позволяет разграничить техническое и научное понимание явления, вызванного цифровизацией: с одной стороны, это использование информационно-телекоммуникационных технологий государством в конкретных целях, с другой стороны, это

процесс трансформирования механизма государства, требующий не только соответствующего правового регулирования, но и научной разработки. Так, в широком определении понятия подчеркивается значение электронного государства в изменении деятельности органов государственной власти в лучшую сторону благодаря наибольшей чувствительности к внутренним и внешним эффектам, которая появляется вследствие внедрения информационно-телекоммуникационных технологий, помимо этого, говорится и об улучшении предоставления услуг гражданам, обеспечения их прав.

С одной стороны, можно говорить о процессе перехода от традиционных форм взаимодействия государства с населением к дистанционным, цифровым, рассматривая электронное государство как комплекс средств. С другой стороны, данный переход имеет более глобальное значение, так как затрагивает все функции государства и требует произвести выработку новых методов осуществления государственной власти, основанных на дистанционном взаимодействии через информационные технологии с возможностью интерактивного общения, обратной связи, обратного контроля, механизмов защиты прав личности и т. д.

Информационно-коммуникационные технологии, развиваясь динамично, постепенно проникли во все сферы жизнедеятельности социума, обеспечив качественно новый уровень его развития, повысив комфортность человеческого существования в рамках природной и социальной среды. Но указанные процессы имеют и оборотную сторону: преступники также воспользовались новыми возможностями, которые предоставляют современные технологии. Использование информационно-коммуникационных технологий в преступной деятельности повысило общественную опасность этой деятельности, способствует возрастанию размеров ущерба, наносимого гражданам, юридическим лицам и государству преступниками, освоившими способы применения при совершении противоправных действий возможностей информационно-коммуникационных технологий. В то же время, поскольку большинство интересов человека в настоящее время значительным образом определяются состоянием окружающей их информационной сферы, то целенаправленные или непреднамеренные воздействия на информационную сферу со стороны внешних или внутренних источников представляют собой реальную угрозу безопасности человека и общества.

Следует отметить, что с началом становления и развития информационно-телекоммуникационных технологий происходит повсеместное внедрение их во все сферы жизни общества. Исключением не стали государственные структуры: расширяется применение IT-технологий

в реализации их функций, отмечается смена способа и характера взаимодействия с гражданами на электронно-телекоммуникационный, а также налаживание обратной связи на более высоком уровне. Указанные нововведения являются основными составляющими электронного государства, которые, в свою очередь, имеют соответствующую нормативно-правовую базу. При этом при рассмотрении вопроса реализации положений концепции электронного государства возникает потребность определения того, каким образом государство регулирует внедрение информационно-телекоммуникационных технологий, необходимо проведение анализа законодательства Российской Федерации на предмет регулирования развития идеи электронного государства в действующих нормативно-правовых актах, определения форм и содержания электронного государства в Российской Федерации [2].

В рамках федерального законодательства основным нормативно-правовым актом, регулирующим положения концепции электронного государства, является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]. Данный закон содержит не только ключевые понятия в области информации, но и основные требования к работе с информацией и ответственность за их нарушение.

В рамках стратегии развития информационного общества процессы цифровизации и автоматизации применяются в основном в системах инженерно-технического обеспечения (охранные системы, противопожарные системы, системы регулирования параметров микроклимата и освещенности помещений и т. д.), при этом вопросы обеспечения безопасности (в т. ч. механической) зданий, сооружений, технических устройств и их частей продолжают оставаться в рамках традиционного подхода к оценке качества [4, с. 103]. В связи с этим можно констатировать несоответствие охвата информатизации процессов существующей потребности информационного общества.

Безопасность — положение, при котором не угрожает опасность кому-чему-нибудь, т. е. рассмотрение категории «безопасность» недопустимо безотносительно какого-либо объекта или субъекта [5]. Угроза безопасности информации представляет собой негативное явление преднамеренного или непреднамеренного характера, направленное на хищение, уничтожение или искажение информации. Каждый из данных факторов может являться критичным, если речь идет об информации ограниченного доступа [6].

Следует отметить, что большинство сотрудников органов внутренних дел пользуются оборудованием, с помощью которого возможен выход в информационно-телекоммуникационные сети на программном обеспечении, не гарантирующем полной безопасности осуществляемых действий. Зачастую электронные рабочие места сотрудников базируются на операционной системе Windows, обеспечение защиты субъектов деятельности на которой затруднено. Стоит заметить, что Windows не отечественная операционная система. Это означает, что создание на ней государственных платформ, обеспечивающих цифровую сохранность, затруднено и прослеживается необходимость внедрения отечественного программного обеспечения, позволяющего соответствовать требованиям, критериям для работы.

Тем не менее также существует проблема материально-технического обеспечения сотрудников офисной техникой должного уровня. В большинстве территориальных подразделений органов внутренних дел качество такого оборудования находится на низком уровне, не позволяющем в полной мере функционировать дополнительному программному обеспечению деятельности в должной степени, либо такое оборудование и вовсе отсутствует, в связи с чем также возникает ситуация, при которой часть участников электронного документооборота функционируют в электронной системе, а часть за ее пределами [7, с. 55]. Как правило, это выражается в необходимости распечатать документ, согласовать его письменно, затем отсканировать и обратно загрузить в систему электронного документооборота для прохождения дальнейшей процедуры подписания или согласования документа. В этой связи некоторые авторы утверждают о необходимости единовременного перевода на электронный документооборот всех правоохранительных органов [8, с. 189].

Хищение информации представляет собой целенаправленный процесс, целью которого является именно получение информации, распространение которой может нанести вред, например, репутации человека, финансовому благополучию организации или обороноспособности государства. Хищение возможно предотвратить путем введения комплекса мер для ограничения информации, например таких, как установка систем защиты информации на персональные компьютеры сотрудников; введение организационных мер, направленных на недопущение посторонних лиц на рабочие места; установка технических устройств, препятствующих допуску неавторизированных лиц: например, системы контроля и управления доступом, различные шлагбаумы и т. д. В то время как

уничтожение представляет собой процесс преднамеренной или непреднамеренной ликвидации информации, который возможно нейтрализовать путем введения обязательного резервирования информации критического характера, например, после каждого рабочего дня персональные компьютеры автоматически копируют информацию на сервер.

Искажение информации представляет собой преднамеренную или непреднамеренную подмену информации, что возможно предотвратить путем дублирования или введения избыточности передаваемой информации. Например, при передаче информации, искажение которой будет являться критичным, осуществлять передачу посредством технических средств и почты. Утечка информации представляет собой неконтролируемый процесс ухода информации ограниченного доступа лицам, не допущенным к данной информации. Иначе говоря, информация, не предназначенная для огласки, становится доступной перечню лиц, не допущенных к этой информации.

Различают такие каналы утечки информации, как агентурные и технические. Агентурный канал утечки информации подразумевает вербовку лиц, представляющих интерес в плане добывания различной информации. Для установления контакта с лицом, которое интересно стороне разведки, используются различные психологические приемы. После того, как контакт установлен, принимаются дальнейшие шаги по сближению с объектом и формированию у объекта иллюзии дружеской атмосферы при общении с разведчиком. Далее могут разыгрываться самые различные сценарии, которые направлены лишь на одну цель — на добывание интересующей информации. Например, может быть смоделирована ситуация, что у мнимого друга объекта разведки срочно возникла необходимость передать какой-либо предмет, оставив его в конференц-зале. Ничего не подозревающий объект пронесет предмет с вмонтированным передатчиком и оставит его в конференц-зале, не вызвав подозрений у своих коллег. Сценарии возможны самого различного плана, вплоть до того, что разведчики могут пойти на жертвы ради добывания информации. Более того, они могут быть сами раскрыты и осуждены. Факторами образования технических каналов утечки информации являются: несовершенство (элементов, решений, технологии, монтажа), эксплуатационный износ (изменение характеристик, выход из строя, халатность), злоумышленные действия (перенастройка, авария, блокирование защиты) [9, с. 102].

Наиболее часто на практике встречается электромагнитный канал утечки информации (электромагнитные волны безгранично распространяются и принимаются специальной аппаратурой с последующим

усилением и раскодированием), а также электрический (прямое подключение к линии связи с последующим усилением сигнала), индукционный (регистрируются и усиливаются электромагнитные излучения линий связи), виброакустический (канал утечки возникает за счет преобразования акустических колебаний в электрические сигналы), акустический (речевой сигнал распространяется по воздуху и усиливается), акустоэлектрический (регистрируются колебания строительных конструкций под воздействием акустических), оптико-электронный (изменяются отражающие характеристики стекол под воздействием акустических колебаний) и параметрический (изменяются параметры электронных схем под воздействием акустических колебаний) [10, с. 54].

Одним из актуальных каналов утечки информации является канал высокочастотного навязывания. Идея состоит в том, что злоумышленник, находясь на удаленном расстоянии от объекта разведки, подает высокочастотный импульс на металлосодержащие элементы, например, персональные компьютеры, мониторы, батареи отопления и т. д. Человек, находясь в данном помещении, ведет конфиденциальный разговор, который модулирует высокочастотный сигнал разведчика, который тот, в свою очередь, принимает и демодулирует. Высокая вероятность перехвата информации по данному каналу утечки обусловлена тем, что практически все окружение современного человека имеет элементы, от которых может произойти переизлучение [11, с. 42].

Не менее интересным каналом утечки информации является канал утечки побочных электромагнитных излучений и наводок. Данный канал утечки представляет собой электромагнитный информативный фон от технических устройств обработки информации, который может содержать сведения, которые обрабатываются в данных устройствах. При перехвате данного фона со средних расстояний, например, около 300 метров, возможно восстановить данную информацию с высокой долей вероятности, разместившись, например, на парковке под окнами помещения, в котором обрабатывается информация ограниченного доступа. А наводки возможно снять, подключившись, например, к сети электропитания, единой с той, в которой происходит обработка информации.

Все множество потенциальных угроз безопасности компьютерной системы классифицируются следующим образом. С точки зрения внешнего воздействия угрозы информационной безопасности можно разделить на естественные, то есть те, которые вызваны не человеком, а прямым или косвенным воздействием на компьютерные системы силами природного характера (наводнение, гроза и т. д.), и искусственные,

то есть реализованные человеком. Также угрозы можно классифицировать по источнику воздействия на внутренние угрозы и внешние угрозы. Внутренние угрозы реализуются, как правило, персоналом организации или иными лицами, допущенными к работе в компьютерной системе. Внешние угрозы могут быть реализованы лицом, не имеющим отношения к «атакуемой» организации, преследующим цель нанести определенный ущерб организации путем причинения вреда информационной безопасности [12, с. 226].

Перспективными направлениями совершенствования сферы информационной безопасности, на наш взгляд, представляется создание законодательной базы обеспечения информационной безопасности личности, общества и государства, формирующей правовую основу для противодействия информационным угрозам. Таким образом, меры по обеспечению информационной безопасности страны должны быть комплексными и содержать в себе также и мероприятия идеологического и воспитательного характера, направленные на соответствующую ориентацию общественного сознания.

Список основных источников

1. Путин призвал наращивать в РФ темпы цифровизации [Электронный ресурс] // Телерадиокомпания Вооруженных Сил Российской Федерации «ЗВЕЗДА». — Режим доступа: https://tvzvezda.ru/news/202111121847-Q1TTD.html. — Дата доступа: 12.11.2022.

2. Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года [Электронный ресурс] : приказ М-ва внутр. дел Рос. Федерации, 10 мая 2018 г., № 284 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.

3. Российская газета. — 2006. — 29 июля, № 1652006.

4. Анализ эффективности существующей системы оценки качества материалов, изделий и конструкций на опасных производственных объектах / М. Ю. Наркевич [и др.] // Вестн. МГТУ им. Г. И. Носова. — 2021. — № 2. — С. 103–111.

5. Словарь русского языка / сост. С. И. Ожегов ; под общ. ред. акад. С. П. Обнорского. — 3-е изд. — М. : Гос. изд-во иностранных и нац. словарей, 1953. — 848 с.

6. Смирнов, А. А. Система обеспечения информационной безопасности в Европейском Союзе : моногр. — М. : Всерос. науч.-исслед. ин-т МВД России, 2012. — 163 с.

7. Смирнов, В. М. Правовые акты в сфере информационной безопасности как один из важнейших источников информационной безопасности РФ / В. М. Смирнов, К. А. Перебейнос // Тенденции развития науки и образования. — 2022. — № 85-1. — С. 52–57.

8. Осокин, Р. Б. Электронный документооборот в правоохранительных органах: состояние и проблемы правовой регламентации / Р. Б. Осокин, М. М. Дикажев // Вестн. Моск. ун-та МВД России. — 2020. — № 6. — С. 188–196.

9. Агаев, Р. Ш. Безопасность информационного сопровождения в системе экономической безопасности / Р. Ш. Агаев, Р. Ш. Агаев, А. А. Графов // Нац. безопасность и стратег. планирование. — 2022. — № 2 (38). — С. 98–104.

10. Кучковский, В. А. Педагогические формы обучения информационной безопасности в целях обеспечения экономической безопасности хозяйствующего субъекта / В. А. Кучковский, С. А. Тронин // Управление образованием: теория и практика. — 2022. — № 3 (49). — С. 53–58.

11. Маслова, М. А. К вопросу об угрозах, методах анализа и оценке рисков информационной безопасности АСУ ТП и критической инфраструктуры / М. А. Маслова, В. С. Аверьянов // Информационная безопасность : сб. докл. Всерос. Шк. молодых ученых / Сибир. гос. ун-т телекоммуникаций и информатики. — Новосибирск, 2022. — С. 40–46.

12. Ершова, Е. Е. Информационная безопасность как элемент экономической безопасности / Е. Е. Ершова // Управление образованием: теория и практика. — 2022. — № 6 (52). — С. 225–230.

Certain aspects of information security in the conditions of digitalization of society

Computer technologies have become an integral part of the life of every member of society due to their widespread use. Solving the problems of information security in the conditions of the modern socio-political situation in our country is one of the key tasks of ensuring the vital activity of society, primarily due to the value of information resources at the present time. The competent solution of problems in the field of information security directly depends on the applied security policy: it is necessary to take into account all aspects of the technological process of information processing so that the most vulnerable objects are protected as much as possible when a criminal appears.